PTO/SB/17p (11-05)
Approved for use through 07/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FEE
Under 37 CFR 1.17(f), (g) & (h)
TRANSMITTAL
(Fees are subject to annual revision)

Send completed form to: Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

Application Number	10/678,965
Filing Date	October 2, 2003
First Named Inventor	Oliver et al.
Art Unit	2131
Examiner Name	Matthew T. Henning
Attorney Docket Number	PA3629US

Enclosed is a petition filed under 37 CFR 1.102(d) **that requires a processing fee (37 CFR 1.17(f), (g), or (h)). Payment of $** 130.00 **is enclosed.**

This form should be included with the above-mentioned petition and faxed or mailed to the Office using the appropriate Mail Stop (e.g., Mail Stop Petition), if applicable. *For transmittal of processing fees under 37 CFR 1.17(i), see form PTO/SB/17i.*

Payment of Fees (small entity amounts are NOT available for the petition fees)

[✓] The Commissioner is hereby authorized to charge the following fees to Deposit Account No. 06-0600 :
    [ ] petition fee under 37 CFR 1.17(f), (g) or (h)   [✓] any deficiency of fees and credit of any overpayments
Enclose a duplicative copy of this form for fee processing.

[✓] Check in the amount of $ 130.00 is enclosed.

[ ] Payment by credit card (Form PTO-2038 or equivalent enclosed). Do not provide credit card information on this form.

Petition Fees under 37 CFR 1.17(f):   Fee $400   Fee Code 1462
For petitions filed under:
§ 1.36(a) - for revocation of a power of attorney by fewer than all applicants
§ 1.53(e) - to accord a filing date.
§ 1.57(a) - to accord a filing date.
§ 1.182 - for decision on a question not specifically provided for.
§ 1.183 - to suspend the rules.
§ 1.378(e) - for reconsideration of decision on petition refusing to accept delayed payment of maintenance fee in an expired patent.
§ 1.741(b) - to accord a filing date to an application under § 1.740 for extension of a patent term.

Petition Fees under 37 CFR 1.17(g):   Fee $200   Fee Code 1463
For petitions filed under:
§ 1.12 - for access to an assignment record.
§ 1.14 - for access to an application.
§ 1.47 - for filing by other than all the inventors or a person not the inventor.
§ 1.59 - for expungement of information.
§ 1.103(a) - to suspend action in an application.
§ 1.136(b) - for review of a request for extension of time when the provisions of section 1.136(a) are not available.
§ 1.295 - for review of refusal to publish a statutory invention registration.
§ 1.296 - to withdraw a request for publication of a statutory invention registration filed on or after the date the notice of intent to publish issued.
§ 1.377 - for review of decision refusing to accept and record payment of a maintenance fee filed prior to expiration of a patent.
§ 1.550(c) - for patent owner requests for extension of time in ex parte reexamination proceedings.
§ 1.956 - for patent owner requests for extension of time in inter partes reexamination proceedings.
§ 5.12 - for expedited handling of a foreign filing license.
§ 5.15 - for changing the scope of a license.
§ 5.25 - for retroactive license.

Petition Fees under 37 CFR 1.17(h):   Fee $130   Fee Code 1464
For petitions filed under:
§ 1.19(g) - to request documents in a form other than that provided in this part.
§ 1.84 - for accepting color drawings or photographs.
§ 1.91 - for entry of a model or exhibit.
§ 1.102(d) - to make an application special.
§ 1.138(c) - to expressly abandon an application to avoid publication.
§ 1.313 - to withdraw an application from issue.
§ 1.314 - to defer issuance of a patent.

Kenneth M. Kaslow (signature)	July 17, 2006
Signature	Date
Kenneth M. Kaslow	32,246
Typed or printed name	Registration No., if applicable

OIPE
JUL 2 1 2006
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS:	Oliver et al.
APPLICATION NO.:	10/678,965
FILING DATE:	October 2, 2003
TITLE:	Fraudulent Message Detection
EXAMINER:	Matthew T. Henning
ART UNIT:	2131
ATTY.DKT.NO.:	PA3629US

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postage prepaid, in an envelope addressed to Mail Stop Petition, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on **July 17, 2006.**

Kenneth M. Kaslow

Kenneth M. Kaslow

MAIL STOP PETITION
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

PETITION TO MAKE SPECIAL IN ACCORDANCE WITH

37 C.F.R. § 1.102(D) AND MPEP § 708.02(VIII)

SIR:

The Applicants respectfully request the Examiner advance the present application out of turn for examination (accelerated examination) through the submission of the present petition. This petition is presented in accordance with 37 C.F.R. § 1.102(d) and the conditions set forth for such a petition as detailed in MPEP § 708.02(VIII).

07/24/2006 JBALIMAN 00000007 10678965

01 FC:1464   130.00 OP

1

I. MPEP § 708.02(VIII)

MPEP § 708.02(VIII) notes that "[a] new application (one which has not received any examination by the examiner) may be granted special status." MPEP § 708.02(VIII). The Applicants declare that the present application is new in that it has not received any examination by the examiner and is thus eligible for special status. Granting of special status is respectfully requested.

II. MPEP § 708.02(VIII)(A)

MPEP § 708.02(VIII)(A) requires the applicant "[s]ubmit[ ] a petition to make special accompanied by the fee set forth in 37 CFR 1.17(h)." MPEP § 708.02(VIII)(A). The Applicants submit the present petition to make special by means of accelerated examination. The fee set forth by 37 C.F.R. § 1.17(h) is satisfied by the enclosed check. The Examiner has been authorized to charge any additional fee due to Deposit Account 06-0600 through the enclosed Form PTO-SB-17p, which is presented in duplicate.

III. MPEP § 708.02(VIII)(B)

MPEP § 708.02(VIII)(B) requires "all claims [be] directed to a single invention." MPEP § 708.02(VIII)(B). Alternatively, if all the claims in an application presented for a grant of special status are not directed toward a single invention as determined by the Office, the applicants are required to "make an election without traverse as a prerequisite to the grant of special status." MPEP § 708.02(VIII)(B). The Applicants believe that all claims presented in this application are directed to a single invention. If the Office makes a determination that the claims are not directed toward a single invention, the Applicants will make an election without traverse.

IV.   MPEP § 708.02(VIII)(C)

The Applicants hereby declare that a pre-examination search has been made as required by MPEP § 708.02(VIII)(C). The pre-examination search was directed toward the invention as claimed in the application and in the following fields:

A.   United States Patent and Trademark Office Full-Text Database

The United States Patent and Trademark Office Full-Text database for both issued patents and pending publications was searched in the following classes and subclasses:

- Class 380, Subclass 1 for Cryptography; Cryptanalysis;
- Class 380, Subclass 2 for Cryptography; Equipment Test or Malfunction Indication;
- Class 700, Subclass 55 for Data Processing: General Control Systems or Specific Applications; Filtering;
- Class 707, Subclass 6 for Data Processing: Database and File Management or Data Structures; Pattern Matching Access;
- Class 707, Subclass 7 for Data Processing: Database and File Management or Data Structures; Sorting;
- Class 708, Subclass 306 for Electrical Computers: Arithmetic Processing and Calculating; Finite Arithmetic Effect;
- Class 708, Subclass 525 for Electrical Computers: Arithmetic Processing and Calculating; Status Condition/Flag Generation or Use;
- Class 708, Subclass 530 for Electrical Computers: Arithmetic Processing and Calculating; Error Detection or Correction;
- Class 726, Subclass 22 for Information Security; Monitoring or Scanning of Software or Data Including Attack Prevention;
- Class 726, Subclass 23 for Information Security; Intrusion Detection;
- Class 726, Subclass 24 for Information Security; Virus Detection;
- Class 726, Subclass 25 for Information Security; Vulnerability Assessment;

B. European Patent Office esp@cenet Database

The European Patent Office's esp@cenet classification database for both issued patents and pending applications was searched in the following European Classifications (ECLA):

- H04L12/58F for Electricity; Electric Communication Technique; Transmission of Digital Information; Data Switching Networks; Stored and Forward Switching Systems; Message Switching Systems with Filtering and Selective Blocking Capabilities;

C. The World Intellectual Property Office's

The World Intellectual Property Organization's PatentScope database for published international applications was search in the following International Patent Classifications (IPC):

- G06F for Physics; Computing, Calculating, Counting; Electrical Digital Data Processing;

D. The Japanese Patent Office

The Japanese Patent Office 'Patent Abstracts of Japan' database for both issued patents and pending applications was searched in the following IPC:

- G06F for Physics; Computing, Calculating, Counting; Electrical Digital Data Processing;

E. The Association of Computing Machinery's (ACM) Digital Library

The ACM Digital Library database for articles referring to 'spam,' 'unsolicited commercial e-mail' (and certain variants (*e.g.*, 'UCE')), and 'phishing';

F. The Internet Search Engine 'Google'

The Internet Search Engine 'Google' (http://www.google.com) was queried with respect to the search language 'phish' and 'phishing.'

4

G.   International Search Report

References identified in the International Search Report for Patent Cooperation Treaty Application No. PCT/US2004/025438, which is related to the present application, have been provided in an *Information Disclosure Statement*. The Applicants note that certain references identified in the International Search Report are *not* prior art references with respect to priority dates and are therefore not discussed in the course of the present petition.

H.   References Provided by the Applicants

Certain references identified by the Applicants have been previously provided in an *Information Disclosure Statement*. These references have been carefully reviewed and have been determined to be, by far, less relevant and/or cumulative with respect to the references discussed in the context of MPEP § 708.02(VIII)(E). Notwithstanding, these references are identified below.

V.   MPEP § 708.02(VIII)(D)

The references deemed most closely related to the subject matter encompassed by the claims (and a copy thereof in the case of any foreign or non-patent literature) have been submitted to the U.S. Patent Office in an *Information Disclosure Statement* submitted on July 17, 2006.

VI.   MPEP § 708.02(VIII)(E)

The Applicants submit, herewith, a detailed discussion of the references, which points out in the particularity requirement by 37 C.F.R. § 1.111(b) and (c). Said discussion identifies how the claimed subject matter is patentable over the references identified herein.

U.S. 5,903,830: *Transaction Security Apparatus and Method* (Joao et al.)

Joao et al. purportedly provides "an apparatus and a method for providing financial transaction authorization, notification and/or security." 830:3:62-64. More specifically, Joao et al. purports to provide "an apparatus and a method for providing financial transaction authorization, notification and/or security in conjunction with credit card, charge card, debit card, and/or currency or 'smart' card use, savings and/or checking account activity and use and/or cellular telephone use." 830:3:64-4:2.

Joao et al. includes "a point-of-sale authorization terminal . . . [located] in various establishments and which are utilized in conjunction with the sale of goods and/or services and/or in other types of financial transactions." 830:4:7-11. These terminals "may be utilized at the location of the seller and/or service provider" or "the point-of-sale terminal may be located at the site of the goods or service provider or vendor, such as in cases when the sale is a telephone order, mail order and/or other type of transaction." 830:4:11-16. Joao et al. notes that the apparatus may be applicable to "transactions made on, or over, the INTERNET and/or other on-line services or communication networks or mediums." 830:4:16-18.

A "central processing computer," in Joao et al. "may service any predefined group of card holders and/or any pre-defined group(s) and/or type(s) of cards." 830:4:23-25. Joao et al.'s "central processing computer may also process accounts for any of the various banks and/or financial institutions which issue and/or manage credit cards, charge cards, debit cards and/or currency or 'smart' cards and/or process or manage these accounts." 830:4:25-30. Upon presentation of any of the aforementioned transaction cards, "[t]he central processing computer will then process the information and/or data pertinent to the transaction and to the particular card account and may request, if needed, that the point-of-sale operator enter the transaction amount." 830:5:39-42. The central processing unit then "determine[s] if the card has been lost, stolen and/or cancelled and/or de-activated." 830:5:45-46. The central processing computer in Joao et al. may also "perform a test in order to determine if the maximum

credit, charge or debit account limit has been exceeded and/or if the card has been depleted of its currency value." 830:5:47-50.

If an indication of the transaction card having been lost, stolen, cancelled, and so forth is not provided, the central processing computer "may then . . . transmit respective signals and/or data to any one or more of the cardholder's designated fax machine, personal computer, telephone, telephone answering machine, alternate telephone, alternate telephone answering machine, network computer, and/or alternate beeper or pager, either sequentially and/or simultaneously." 830:6:11-17. This transmitted information may include "information and/or data identifying the transaction and may include the name of the store or the service provider and the amount of the transaction" in addition to "the time of the transaction, the location (i.e. city, town, village, state, country, etc.) of the transaction." 830:6:19-21; 22-24. The information and/or data may also include the phone number of the central processing office and/or computer servicing the account so that the cardholder may telephone same in order to authorize or cancel the transaction." 830:6:24-28. The cardholder "may either utilize the reply or two-way pager feature on [a] communication device in order to either approve, or authorize, the transaction or to disapprove, or void the transaction." 830:6:46-49.

With respect to independent claim 1, Joao et al. fails to disclose 'a method for classifying a message.' Joao et al. concerns a cardholder approving or authorizing a transaction taking place with respect to the cardholder's transaction card; no message is classified. As Joao et al. does not disclose a message for classification, there is not a 'plurality of reference points' that are extracted from the message and subsequently classified. As the classification of a plurality reference points is absent from Joao et al., there is no determination that the message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Joao et al. thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, Joao et al. again fails to disclose 'a method for classifying a message.' Joao et al. also fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. Joao et al. thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, Joao et al. does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, Joao et al. does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

U.S. 5,987,440: *Personal Information Security and Exchange Tool* (O'Neil et al.)

O'Neil et al. concerns a purported "software system . . . with supporting applications operating on an individual user's personal computer system, inclusive of wire-line and wireless tele-computing devices" and "directed to a system for allowing an individual or entity to protect, command, control, and process personal information on a computer network, including the Internet." 440:2:2-5; 2:6-8. Through the aforementioned software system, a "member can assign access rules to each piece of personal information. These access rules set the requirements that must be met before an individual piece of information can be processed." 440:2:35-38.

Upon a request for access to information, an electronic broker "checks to see if the requester and the situation meet the requirement of the rule. If so, the E-Broker allows the requested information to be processed; if not, the E-Broker does not allow the information to be processed." 440:2:45-48. "Using . . . transitive privilege rules, a member can maintain command and control on third party dissemination and

8

processing of their personal information." 440:2:52-55. "A member may also create an agent . . . to interact with other members." 440:2:56-57.

With respect to independent claim 1, O'Neil et al. fails to disclose 'a method for classifying a message.' O'Neil et al. concerns a community of access settings to prevent unauthorized access to information; no message is classified. As O'Neil et al. does not disclose a message for classification, there is no 'plurality of reference points' that are extracted from the message and subsequently classified. As the classification of a plurality reference points is absent from O'Neil et al., there is no determination that the message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. O'Neil et al. thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, O'Neil et al. again fails to disclose 'a method for classifying a message.' O'Neil et al. also fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. O'Neil et al. thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, O'Neil et al. does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, O'Neil et al. does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

U.S. 6,122,740: *Method and Apparatus for Remote Network Access Logging and Reporting* (Andersen)

Andersen describes a purported "method and apparatus for remote network access logging and reporting" whereby "individuals [are not allowed] to access systems other than those they are supposed to be accessing." 740:1:46-47; 1:21-22. "Temporary access list 235 is a list of host systems which are not to be accessed by the user of the system. Alternatively, access list 235 may be a list of only those systems which can be accessed by the user." 740:5:35-39. In one embodiment, "access list 235 is obtained from log server 150 and is stored in volatile memory . . . . [D]ata in temporary access list 235 could also be encrypted in any of a wide variety of conventional manners, and decrypted by logging [dynamic link library] DLL 230 whenever accessed." 740:5:38-46.

"Once the access list is retrieved, the logging DLL is able to receive requests from a user . . . to access a host system." 740:6:14-16. The DLL "compares the host system to the locally stored access list . . . [and] checks whether the request conflicts with the access list." 740:6:17-19. "If the request does not conflict with the access list, then the logging DLL forwards the request to the host system . . . . [I]f the request does conflict with the access list, then the logging DLL sends log data for the request to the logging server . . . as well as forwarding the request to the host system." 740:6:19-25. "[T]his log data can include any of a wide range of data including the identification of the requested host system, the date and time of the request, etc." 740:6:26-28.

With respect to independent claim 1, Andersen fails to disclose 'a method for classifying a message.' Andersen concerns preventing unauthorized access to a particular computing system; no message is classified. As Andersen does not disclose a message for classification, there are no 'plurality of reference points' that are extracted from the message and subsequently classified. As the classification of a plurality reference points is absent from Andersen there is no determination that the message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the

10

method of independent claim 1. Andersen thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, Andersen again fails to disclose 'a method for classifying a message.' Andersen also fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. Andersen thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, Andersen does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, Andersen does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

U.S. 5,982,890: *Method & System for Detecting Fraudulent Data Update* (Akatsu)

Akatsu purports to provide "a method and system for detecting fraudulent or unauthorized data update by insiders of databases of a distributed computer system, capable of allowing third parties to check fraud." 890:1:32-25. Akatsu discloses "distributed databases and local computers at local sales offices and local business offices" in addition to a "monitor computer, and a network interconnecting the local and monitor computers." 890:1:39-40; 1:14-42. The monitor computer "generat[es] parity data of initial data collected from respective sites of the databases at each of same storage fields and storing the generated parity data." 890:1:43-45. "[E]ach time data in each database is updated, new parity data from data before and after the update and old parity data [is generated] to replace the old parity data by the new parity data." 890:1:46-49.

11

The monitor computer then "compare[s] parity data generated at an auditing time from latest data stored in the databases at each of the same storage fields, with the parity data already stored" and determines "if the comparison result indicates an inconsistency of both the parity data, that data in the databases was updated fraudulently." 890:1:49-51; 1:52-54. "If the data in the distributed databases is not coincident with the corresponding data already transmitted to the monitor computer, both the parity data are inconsistent so that fraudulent data update can be detected." 890:1:55-58.

With respect to independent claim 1, Akatsu fails to disclose 'a method for classifying a message.' Akatsu concerns detecting fraudulent data updates; no message is classified. As Akatsu does not disclose a message for classification, there is no 'plurality of reference points' that are extracted from the message and subsequently classified. As the classification of a plurality reference points is absent from Akatsu there is no determination that the message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Akatsu thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, Akatsu again fails to disclose 'a method for classifying a message.' Akatsu also fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. Akatsu thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, Akatsu does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, Akatsu does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

U.S. 6,321,338: *Network Surveillance* (Porras et al.)

Porras et al. purports to provide "a method of network surveillance includ[ing] receiving network packets (e.g., TCP/IP packets) handled by a network entity and building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets that monitors data transfers, errors, or network connections." 338:1:44-49. "A comparison of at least one long-term and at least one short-term statistical profile is used to determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity." 338:1:49-54.

Porras et al. describes "responding [to the comparison] based on the determining whether the difference between a short-term statistical profile and a long-term statistical profile indicates suspicious network activity." 338:1:66-2:2. Responses may include "altering analysis of network packets and/or severing a communication channel" or "transmitting an event record to a network monitor, such as hierarchically higher network monitor and/or a network monitor that receives event records from multiple network monitors." 338:2:2-4; 2:4-7.

Porras et al. also describes "[a] signature engines 24 [that] can detect, for example, address spoofing, tunneling, source routing, SATAN attacks, and abuse of ICMP messages ('Redirect' and 'Destination Unreachable' messages in particular)." 338:7:43-46. The signature engine 24 may utilize threshold analysis, which (according to Porras et al.) is "a rudimentary, inexpensive signature analysis technique that records

13

the occurrence of specific events and, as the name implies, detects when the number of occurrences of that event surpasses a reasonable count." 338:7:47-50. The signature engine 24 of Porras et al. "can also examine the data portion of packets in search of a variety of transactions that indicate suspicious, if not malicious, intentions by an external client" by "pars[ing] FTP traffic traveling through the firewall or router for unwanted transfers of configuration or specific system data, or anonymous requests to access non-public portions of the directory structure." 338:7:55-57; 7:58-62. Porras et al. also describes "[m]onitors 16a-16f [that] may invoke probes in an attempt to gather as much counterintelligence about the source of suspicious traffic by using features such as traceroute or finger." 338:12:15-18.

With respect to independent claim 1, Porras et al. fails to disclose 'a method for classifying a message.' Porras et al. concerns monitoring various network behaviors and identifying suspicious activity but no message appears to be classified. As Porras et al. does not disclose a message for classification, there can be no (and is not) 'plurality of reference points' that are extracted from the message and subsequently classified. As the classification of a plurality reference points is absent from Porras et al. there is no determination that the message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Porras et al. thereby fails to disclose the limitations of claim 25 for at least the same reasons as claim 1.

With respect to independent claim 15, Porras et al. again fails to disclose 'a method for classifying a message.' Porras et al. also fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. While Porras et al. does discuss theshhold analysis, there is (1) no indication that this threshold analysis is necessarily equivalent to the Applicant's presently claimed statistical analysis and (2) no showing that any analysis (threshold or statistical) occurs with respect to the aforementioned fraud indicators. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the

14

method of independent claim 15. Porras et al. thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, Porras et al. does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, Porras et al. does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

U.S. 6,334,121: *Usage Pattern Based User Authenticator* (Primeaux et al.)

Primeaux et al. purports to "provide support to system administrators in limiting the ability of unauthorized users to disrupt system operations by monitoring and reporting abnormal user usage patterns." 121:2:40-44. This support supposedly includes "a method that will prevent a destructive command from being executed" whereby "[s]everal commands for each of the system users are tracked" and "[a] combination of security rules and user usage patterns are used to flag suspicious activity on the system." 121:2:45-56; 2:46-47; 2:47-49.

Primeaux et al. exemplifies this supposed method whereby "if a typical user tries to assign himself 'super user', or root, privileges, the security rules catch this and take appropriate action to limit further damage." 121:2:52-55. These actions by the particular user are "then logged to a system security file that the system administrator will review or other appropriate action is taken automatically." 121:2:55-57. Primeaux et al. notes that a supposed "unique advantage of the invention is that it can prevent previously authorized users from executing destructive commands by detecting unusual patterns in their usage of the system." 121:2:57-60. Primeaux et al. further describes "incorporate[ing] machine learning techniques into the method." 121:2:61-62.

With respect to independent claim 1, Primeaux et al. fails to disclose 'a method for classifying a message.' Primeaux et al. concerns monitoring various user activities including assignment of privileges in light of various security rules but no message is ever classified. As Primeaux et al. does not disclose a message for classification, there can be no (and is not) 'plurality of reference points' that are extracted from the message and subsequently classified. As the classification of a plurality reference points is absent from Primeaux et al. there is no determination that the message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Primeaux et al. thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, Primeaux et al. again fails to disclose 'a method for classifying a message.' Primeaux et al. also fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. While Primeaux et al. does discuss application of security rules, there is no indication that this application is (1) necessarily equivalent to the Applicant's presently claimed statistical analysis and (2) that any such rule application occurs with respect to the aforementioned fraud indicators. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. Primeaux et al. thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, Primeaux et al. does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, Primeaux et al. does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to identify a plurality of fraud indicators,' which are

16

subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

U.S. 2003/0172166: *Systems & Methods for Enhancing Electronic Communication Security* **(Judge et al.)**

Judge et al. "relates to computer-based systems and methods for assessing security risks associated with electronic communications transmitted over a communications network." [0002]. Judge et al. describes "[i]ntrusion detection systems (IDS) [that] are being deployed throughout corporate networks." [0017]. The "IDS act like a video camera" and can supposedly "monitor network traffic for suspicious patterns of activity, and issue alerts when that activity is detected." [0017].

Judge et al. notes that "[m]ost e-mail and Web requests and responses are sent in plain text" "include[ing] the e-mail message, its header, and its attachments." [0025]. Additionally, according to Judge et al., "when you dial into an Internet Service Provider (ISP) to send or receive e-mail messages, the user ID and password are also sent in plain text, which can be snooped, copied, or altered." [0025].

Judge et al. describes an assessment strategy including "[a]pplication specific anti-virus protection and anti-spam protection . . . provid[ing] support for screening application specific communications for associated viruses and/or spam." [0070]. "A data collection process occurs that applies one or more assessment strategies to the received communication." [0075]. "The application of each assessment, or the assessments in the aggregate, generates one or more risk profiles associated with the received communication." [0075]. "The collected data may be used to perform threat analysis or forensics," which "may take place after the communication is already received and forwarded." [0075].

Judge et al. goes on to describe that "[i]n one preferred embodiment, the stored risk profile associated with the received communication is aggregated with data associated with previously received communications of the same type." [0080]. In this way, "[t]his newly aggregate data set is then used in analysis of subsequently received communications of that type." [0080].

According to Judge et al., "[i]f an anomaly is detected, an anomaly indicator signal is output. The outputted signal may include data identifying the anomaly detected and the communication in which the anomaly was detected." [0081]. Judge et al. also notes that "[i]nstead of or in addition to a notification, one or more corrective measures could be triggered by the outputted signal" including "refusing acceptance of further communications from the source of the received communication, quarantining the communication, stripping the communication so that it can be safely handled by the application server, and/or throttling excessive numbers of incoming connections per second to levels manageable by internal application servers." [0084].

With respect to independent claim 1, Judge et al. does not disclose the extraction of a 'plurality of reference points' from a message that are subsequently classified. While Judge et al. does assign risk profiles, there is no discussion of a reference point being classified with respect to arriving at a determination that a particular message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Judge et al. thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, Judge et al. fails to disclose 'fraud indicators' in a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. While Judge et al. does reference the aforementioned risk profile, there is no indication that this profile is (1) necessarily equivalent to the Applicant's presently claimed statistical analysis (2) nor that it occurs with respect to the aforementioned fraud indicators. Independent claim 28 concerns a 'computer program product' for

18

'classifying a message' that is similar in scope to the method of independent claim 15. Judge et al. thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, Judge et al. does not disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, Judge et al. does not disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

U.S. 6,938,167: *Using Trusted Communication Channel to Combat User Name/Password Theft* (Roskind)

Roskind suggests that with regard to on-line security, "there are three classes of identification: What you have; What you know; and What you are." 167:2:14-18. Roskind notes that "[m]odern authentication theory suggests that two out of these three classes of identification are needed for significant assurance of identity" and that "[t]he invention recognizes this aspect of security theory and uses the concept of tagging and verification to prevent forged authentication, such as stolen passwords." 167:2:39-41; 167:2:41-44. In this regard, Roskind specifically notes that "[i]t is difficult, if not almost impossible, to prevent spoofing of official pages, for example where innocent victims are lured into supplying user names and passwords." 167:2:45-47.

Roskind seeks to avoid these incidents through "the provisions of online services . . . to make an immediate machine-to-human connection to the most likely valid user." 167:2:48-50. Through the "use [of] a time-varying password generation scheme, such as secure ID, to generate a random number as a function of the time and day, provides assurance that an attacker must immediately use a compromised password." 167:2:51-54. Roskind also notes that "[b]ecause most passwords are compr[om]ised while the users are still online, the invention takes advantage of the fact that it is possible to reach the online user." 167:2:56-59.

The purported invention of Roskind thus "comprises technology for defining a machine as being a machine having enhanced trust, wherein a messaging technology is used to make immediate contact with the user on the enhanced trust system." 167:3:15-18. "[T]he invention provides a mechanism that can contact the compromised user and ask for confirmation for results, i.e. to change a password or even to login, with regard to a reduced trust machine." 167:3:19-22. Through an enhanced trust machine, "even if an attacker steals a password, the true user on the enhanced trust machine is able to preclude a login or preclude a password change." 167:3:22-25.

With respect to independent claim 1, Roskind does not disclose the extraction of a 'plurality of reference points' and subsequent classification of those points, those points having been extracted from a message to be classified. Roskind seeks to establish an instantaneous link with an authorized user with respect to a Secure ID. Roskind concerns maintaining password security and not arriving at a determination that a particular message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Roskind thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, Roskind again fails to disclose 'a method for classifying a message.' Roskind also fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. Roskind's Secure ID is concerned with preventing fraud but not disclose fraud indicators nor statistical analysis of those indicators. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. Roskind thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, Roskind does not disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to

independent claim 27, Roskind does not disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

U.S. 2003-0088627: *Intelligent SPAM Detection System Using an Updateable Nerual Analysis Engine* (Rothwell et al).

Rothwell et al. purports to provide "[a] system, method and computer program product are provided for detecting an unwanted message." [0009]. Through Rothwell et al., "an electronic mail message is received" and "[t]ext in the electronic mail message is decomposed." [0009]. "Statistics associated with the text are gathered using a statistical analyzer" and "[a] neural network engine coupled to the statistical analyzer is taught to recognize unwanted messages based on statistical indicators." [0009]. "The statistical indicators are analyzed utilizing the neural network engine for determining whether the electronic mail message is an unwanted message." [0009].

Rothwell et al. suggests that its "neural network engine can be taught to recognize unwanted messages" whereby "examples are provided to the neural network engine"; "[t]he examples are of wanted messages and unwanted messages." [0010]. "Each of the examples is processed with statistics by the neural network engine for generating weights for the statistics. Each of the weights is used to denote wanted and unwanted messages." [0010]. "Logic associated with the neural network engine is updated based on the processing by the neural network engine." [0010]. "[T]he neural network engine [may] utilize[ ] adaptive linear combination for adjusting the weights." [0014].

Rothwell et al. is further purportedly capable of updating the neural network engine to "recognize an unwanted message"; that "message is identified as an unwanted message," "[t]he features of the message that make the message unwanted are identified" and those "identified features are stored and used by the neural network to identify subsequent unwanted messages." [0014]. The neural network engine, according to Rothwell et al., may also "determine patterns in statistics and words, and

use these to determine whether the message is SPAM based on comparing the patterns to patterns predetermined to be SPAM or non-SPAM." [0040]. "The greater the number of variables in the statistics table, the easier it is for the Artificial Intelligence engine (AI) to 'learn' to differentiate between SPAM and genuine messages." [0040].

With respect to independent claim 1, Rothwell et al. does not disclose the extraction of a 'plurality of reference points' and subsequent classification of those points, those points having been extracted from a message to be classified. While Rothwell et al. discloses decomposing text in a message, there is no suggestion that reference points are identified as required by claim 1. Further, Rothwell et al. only discussed identification of unwanted message and not that a particular message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. Rothwell et al. therefore fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, Rothwell et al. fails to disclose 'fraud indicators' in a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. Decomposing a message does not necessarily arise to identification of fraud indicators and determining that the message itself is 'fraudulent.' Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. Rothwell et al. therefore fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, Rothwell et al. does not disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, Rothwell et al. does not disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

22

FBI Press Release: *FBI Says Web 'Spoofing' Scams are a Growing Problem*

The FBI Press Release notes that "[b]ogus e-mails that try to trick customers into giving out personal information are the hottest, and most troubling, new scam on the Internet." These e-mails are "contributing to a rise in identity theft, credit card fraud, and other Internet frauds." "'Spoofing,' or 'phishing' frauds attempt to make Internet users believe that they are receiving e-mail from a specific, trusted source . . . when that is not the case."

E-mail spoofing involves "the header of an e-mail" that "appears to have originated from someone or somewhere other than the actual source." IP spoofing "is a technique used to gain unauthorized access to computers, whereby the intruder sends a message to a computer with an IP address indicating that the message is coming from a trusted port." Link alteration "involves altering the return address in a web page sent to a consumer to make it go to the hacker's site rather than the legitimate site."

The FBI Press Release suggests "exercise[ing] extreme caution" "[i]f you encounter an unsolicited e-mail that asks you . . . for personal financial or identity information." The FBI Press Release further suggests "report[ing] fraudulent or suspicious e-mail to your ISP" and to "[l]ook for the lock at the bottom of your browser and 'https' in front of the website address." The FBI Press Release also advises "tak[ing] note of the header address on the web site."

With respect to independent claim 1, the FBI Press Release fails to disclose 'a method for classifying a message.' The FBI Press Release concerns the proliferation of phishing. The FBI Press Release does not disclose means or a methodology for classifying a message and, as such, there can be (and is not) a 'plurality of reference points' that are extracted from the message and subsequently classified. As the classification of a plurality reference points is absent from the FBI Press Release there is no determination that the message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. The FBI Press Release

thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, the FBI Press Release again fails to disclose 'a method for classifying a message.' The FBI Press Release also fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. The FBI Press Release thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, the FBI Press Release does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, the FBI Press Release does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

'Wired': *Cloaking Device Made for Spammers*

The 'Wired' article notes that "spammers . . . [may] create websites that are essentially untraceable." 'Invisible Bulletproof Hosting' may "protect a site from network sleuthing tools used by spam opponents such as traceroute and whois." "Bulk e-mails and scam artists [have] beg[u]n utilizing the services of crackers who control large networks of compromised computers" "to host porn and credit card phishing sites." The 'Wired' article notes that "[o]ne strategy for mitigating the invisible-hosting problem . . . would be for Internet service providers or domain registrars to blacklist the DNS servers used by such outfits, effectively cutting them off the Internet."

24

With respect to independent claim 1, the 'Wired' article fails to disclose 'a method for classifying a message.' The 'Wired' article concerns tools used by spammers to engage in phishing such as 'invisible hosting.' The 'Wired' article does not disclose classifying a message and, as such, there are no 'plurality of reference points' that are extracted from the message and subsequently classified. As the classification of a plurality reference points is absent from the 'Wired' article there is no determination that the message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. The 'Wired' article thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, the 'Wired' article again fails to disclose 'a method for classifying a message.' The 'Wired' article fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. The 'Wired' article thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

With respect to independent claim 25, the 'Wired' article does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, the 'Wired' article does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

25

Communications of the ACM: *The Homograph Attack*

The ACM article references efforts to obscure the identity of a provider of fraudulent content by "referr[ing] to [a] phony site by its numerical IP address rather than by name, and thus obscure[ing the site's] true identity." The ACM article references that "[a] stronger variant of this hoax might have used a domain named bl00mberg.com." The ACM article further references "[a] new initiative, promoted by a number of Internet standards bodies including IETF and IANA, [that] allows one to register domain names in national alphabets." The ACM article sets forth a concern that "[w]ith the proposed infrastructure in place, numerous English domain names may be *homographed*—maliciously misspelled by substitution of non-Latin letters."

With respect to independent claim 1, the ACM article fails to disclose 'a method for classifying a message.' The ACM article concerns fraudulently identifying a website through the user of IP addresses, interchanging letters/numbers in a domain name, and the use of foreign alphabet letter equivalents. The ACM article does not disclose classifying a message and, as such, there is no 'plurality of reference points' that are extracted from the message and subsequently classified. As the classification of a plurality reference points is absent from the ACM article there is no determination that the message is a 'phish message' as is recited in claim 1. Independent claim 26 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 1. The ACM article thereby fails to disclose the limitations of claim 26 for at least the same reasons as claim 1.

With respect to independent claim 15, the ACM article again fails to disclose 'a method for classifying a message.' The ACM article fails to disclose 'fraud indicators' in such a message thereby preventing 'applying a statistical analysis on the plurality of fraud indicators' such that the analysis reflects that a message is a fraudulent message. Independent claim 28 concerns a 'computer program product' for 'classifying a message' that is similar in scope to the method of independent claim 15. The ACM article thereby fails to disclose the limitations of claim 28 for at least the same reasons as claim 15.

26

With respect to independent claim 25, the ACM article does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to extract a plurality of reference points,' which are subsequently classified for the purpose of 'detecting that the message is a phish message.' With respect to independent claim 27, the ACM article does not disclose a system for 'classifying a message,' nor does it disclose a processor 'configured to identify a plurality of fraud indicators,' which are subsequently analyzed for the purpose of 'determining whether the message is a fraudulent message.'

Other References

The following references were carefully reviewed and determined to be, by far, less relevant and/or cumulative with respect to the references discussed above:

Patent/Publication No.	Publication Date	Patentee/Inventor
6112227	08-29-2000	Heiner
6199102	03-06-2001	Cobb
6650890	11-18-2003	Irlam et al.
2003/0233418	12-18-2003	Goldman
2004/0024639	02-05-2004	Goldman
2004/0158554	08-12-2004	Trottman
2005/0055410	03-10-2005	Landsman et al.
6941348	09-06-2005	Petry et al.
2005/0257261	11-17-2005	Shraim et al.

Non-Patent Literature Title	Author	Date
"Pricing via Processing or Combating Junk Mail"	DWORK	1992
"How to Make Sure a Human is Sending You Mail"	SKOLL	1996
"My Spamblock"	BYRNE	1997
"To Mung or Not to Mung"	GUILMETTE	1997
"Majordomo FAQ"	--- ---	2001
"Spam Foe Needs Filter of Himself"	LANGBERG	April 5, 2003
"In-Boxes that Fight Back"	MCCULLAGH	May 19, 2003
"Viking-12 Junk E-Mail Blocker"	TEMPLETON	July 15, 2003
"Characteristics and Responsibilities Involved in a Phishing Attack"	MERWE	2005
"Protecting Users Against Phishing Attacks with AntiPhish"	KIRDA	2005

VII. Conclusion

The Applicants believe that this Petition to Make Special has met all requirements set forth by 37 C.F.R. § 1.102(d) and MPEP § 708.02(VIII) and respectfully request the petition be granted.

Respectfully submitted,
Jonathan Oliver et al.

July 17, 2006 By: *Kenneth M. Kaslow*

Kenneth M .Kaslow, Reg. No. 32,246
Carr & Ferrell *LLP*
2200 Geng Road
Palo Alto, California 94303
Phone (650) 812-3400
Fax (650) 812-3444